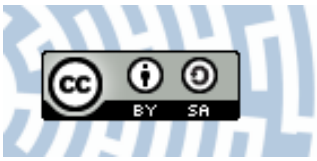
re-BUS

You have downloaded a document from
RE-BUŚ
repository of the University of Silesia in Katowice

Title: Wybrane aspekty praktyczne zapewnienia bezpieczeństwa bibliotecznych systemów informacyjnych w świetle obowiązujących norm

Author: Andrzej Koziara, Agnieszka Jezierska

Citation style: Koziara Andrzej, Jezierska Agnieszka. (2015). Wybrane aspekty praktyczne zapewnienia bezpieczeństwa bibliotecznych systemów informacyjnych w świetle obowiązujących norm. "Bibliotheca Nostra. Śląski Kwartalnik Naukowy" (2015, nr 4, s. 67-80).



Uznanie autorstwa - Na tych samych warunkach - Licencja ta pozwala na kopiowanie, zmienianie, rozprowadzanie, przedstawianie i wykonywanie utworu tak długo, jak tylko na utwory zależne będzie udzielana taka sama licencja.

UNIWERSYTET ŚLĄSKI W KATOWICACH
Biblioteka Uniwersytetu Śląskiego
Ministerstwo Nauki i Szkolnictwa Wyższego

Bibliotheca Nostra.
Śląski Kwartalnik Naukowy
nr 4 (42) 2015, s. 67-80

Andrzej Koziara
Biblioteka Uniwersytetu Śląskiego w Katowicach

Agnieszka Jezierska
Uniwersytet Śląski w Katowicach, Dział Audytu

Wybrane aspekty praktyczne zapewnienia bezpieczeństwa bibliotecznych systemów informacyjnych w świetle obowiązujących norm

Współczesny świat ze swoimi rozwiązaniami prawnymi wymaga od zarządzających podejmowania takich działań, by instytucje przez nich kierowane realizowały wszystkie cele, do których zostały powołane. Realizacja zadań, jakie zostają im przydzielone, zawsze zależna jest od sposobu zarządzania oraz użytych do niego instrumentów. Dobór tych elementów, według naszej oceny, jest szczególnie ważny dla instytucji, które, tak jak biblioteki akademickie, stanowią jedną z agend dużych organizacji, pełniąc w nich funkcje wspomagające. Prawidłowe wypełnianie zadań jest zależne nie tylko od samych jednostek, lecz także od sposobu organizacji całej instytucji. Ma to istotne znaczenie zwłaszcza w miejscach, które w działalności nie wykorzystują zasad opisanych w normie PN-EN ISO 9001 „Systemy zarządzania jakością". Zasady te, jakże ogólne, pozwalają instytucji na uporządkowanie wszystkich procesów zarządczych. Odnoszą się również do zapisów prawnych i normatywnych dotyczących bezpieczeństwa informacji. To właśnie one są źródłem przeświadczenia wszystkich osób zajmujących się systemami bezpieczeństwa, że tylko samodzielne przygotowanie takich systemów jest w pełni efektywne i adekwatne do rzeczywistych potrzeb instytucji. Powodów tego zjawiska jest kilka, a staną się one oczywiste w miarę omawiania kolejnych elementów systemów bezpieczeństwa organizacji. Jako podstawę prawną i normatywną przyjmiemy akty skatalogowane w artykule *Bezpieczeństwo danych i systemów informacyjnych w bibliotekach. Przegląd stanu prawnego* (Koziara, Jezierska, 2015).

Celem przeprowadzonych i opisywanych w pracy badań jest wyodrębnienie najważniejszych, zdaniem autorów, struktur decydujących o skuteczności przygotowanych i wdrożonych systemów bezpieczeństwa informacji. Wiadomości są wyselekcjonowane i uporządkowane z uwagi na adresata – skierowane są głównie do osób, od których w praktyce zależy poziom

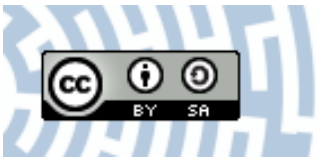
re-BUS

You have downloaded a document from
RE-BUŚ
repository of the University of Silesia in Katowice

Title: Wybrane aspekty praktyczne zapewnienia bezpieczeństwa bibliotecznych systemów informacyjnych w świetle obowiązujących norm

Author: Andrzej Koziara, Agnieszka Jezierska

Citation style: Koziara Andrzej, Jezierska Agnieszka. (2015). Wybrane aspekty praktyczne zapewnienia bezpieczeństwa bibliotecznych systemów informacyjnych w świetle obowiązujących norm. "Bibliotheca Nostra. Śląski Kwartalnik Naukowy" (2015, nr 4, s. 67-80).



Uznanie autorstwa - Na tych samych warunkach - Licencja ta pozwala na kopiowanie, zmienianie, rozprowadzanie, przedstawianie i wykonywanie utworu tak długo, jak tylko na utwory zależne będzie udzielana taka sama licencja.

UNIWERSYTET ŚLĄSKI W KATOWICACH
Biblioteka Uniwersytetu Śląskiego
Ministerstwo Nauki i Szkolnictwa Wyższego

bezpieczeństwa, czyli dyrekcji biblioteki, pracowników średniego szczebla kierowniczego oddziałów merytorycznych, administracji oraz służb informatycznych biblioteki. Przytoczone informacje mogą być również wykorzystywane przez inne jednostki organizacyjne uczelni wyższych lub ich służby informatyczne. Ze względu na uniwersalność poruszanej w artykule problematyki, materiał ten jest również użyteczny dla kadry kierowniczej innych jednostek publicznych, których dotyczy Rozporządzenie Rady Ministrów w sprawie minimalnych wymagań dla systemów teleinformatycznych (Rozporządzenie, 2012), może także zainspirować kadrę kierowniczą instytucji publicznych do czynnego zainteresowania się pozyskaniem wiedzy, niezbędnej do pełnienia roli przywódczej w zakresie zapewnienia bezpieczeństwa informacji.

Na wstępie należy podkreślić, jak istotne jest korzystanie z precyzyjnej terminologii, co nie tylko pozwoli nam przygotować i wdrożyć procedury postępowania, lecz także będzie podstawą do egzekwowania ich realizacji.

Pierwszym i najważniejszym elementem, który musimy określić samodzielnie, jest dostosowana do naszych potrzeb definicja samego pojęcia bezpieczeństwa informacji. Jest ona podstawą wszystkich podejmowanych działań i w przyszłości będzie decydowała o rzeczywistych jego kosztach, liczonych według modelu opisanego przez Gartner Group pod nazwą Total Cost of Ownership (TCO). Najogólniej TCO służy do określania rzeczywistych kosztów informatyki, zawiera nie tylko pieniądze na zakupy urządzeń i oprogramowania, stanowiących część infrastruktury teleinformatycznej, ale także sumy pochodzące z list płac (nie tylko personelu informatycznego) oraz inne ukryte koszty pośrednie i koszty generowane przez przestoje systemów. Ze względu na charakter biblioteki i zadania przez nią spełniane, zastosowanie takiej logiki liczenia kosztów wymaga oczywiście wielu przybliżeń i dokonywania wyceny pracy nie tylko naszego personelu, ale także podjęcia prób określenia ich w stosunku do naszych czytelników. Wydaje się, że zadanie to może być najbardziej skomplikowane, gdyż dla metodyki TCO najważniejszym składnikiem modelu jest baza danych o kosztach informatyki dla poszczególnych branż, a biblioteki, szczególnie wyższych uczelni, są instytucjami, których modele nie mieszczą się w uśrednionych danych statystycznych[1]. Zjawisko to dotyczy tak kosztów pracy personelu, z reguły reprezentującego niszowe specjalności i wykonującego nietypowe działania jak i czytelników, na których zachowanie, a co za tym idzie koszty ich działań, mamy jeszcze mniejszy wpływ. Mimo tych trudności nie powinniśmy rezygnować ze stosowania TCO, gdyż jego najważniejszym przesłaniem jest identyfikacja wszystkich składników kosztów, co dla bezpieczeństwa będzie jednym z najważniejszych kryteriów dokonywania wyborów

[1] Szczegółowo zagadnienie TCO przedstawia: Bujak B. (oprac.). (2013) *The art of IT, czyli o zarządzaniu IT, TCO – czyli zarządzanie całkowitymi kosztami IT*. Pobrane 25.03.2015, z http://tco.pl/?p=746

podczas projektowania, wdrażania i utrzymywania systemów bezpieczeństwa informacji. Na potrzeby tego tekstu będziemy korzystać z wcześniej ustalonych definicji (Koziara, Jezierska, 2015).

Podczas kolejnych działań należy dążyć do przygotowania i wdrożenia Systemu Zarządzania Bezpieczeństwa Informacji (SZBI) zdefiniowanego w normie PN-ISO/IEC 27001:2014-12. Wszystkie czynności podejmowane z SZBI na każdym etapie jego uszczegóławiania oparte będą o zasady działania koła Deminga. Dla osób, które dotąd nie zetknęły się z wydanymi poprzednio normami bezpieczeństwa informacji (Technika informatyczna, 2007a), pojęcie to będzie kojarzyć się tylko z obowiązującą obecnie normą systemów zarządzania jakością. Uważamy, że podejmując po raz pierwszy prace nad SZBI zarządzający instytucją oraz osoby zaangażowane w jego przygotowanie oprócz obecnie obowiązujących rozwiązań normatywnych powinni zapoznać się z poprzednimi wersjami tych norm. W ich treści znajdą bowiem bardzo wiele praktycznych wskazówek postępowania z SZBI. Koło Deminga to model PDCA realizujący zarządzanie zmianami w myśl ciągle powtarzanych działań: Planuj (Plan – ustanowienie obecnej wersji SZBI), Wykonuj (Do – wdrażanie i eksploatacja obecnej wersji SZBI), Sprawdzaj (Check – monitorowanie i przegląd obecnej wersji SZBI) oraz Działaj (Act – utrzymanie i doskonalenie obecnej wersji SZBI) (Technika informatyczna, 2007b; Krawiec, Ożarek, 2014).

Polityka Bezpieczeństwa Informacji

Przygotowanie do wdrożenia SZBI należy rozpocząć od opracowania wstępnej wersji Polityki Bezpieczeństwa Informacji (PBI). Zdarza się, że podczas przygotowania pierwszej wersji PBI osoby ją opracowujące dysponują małą liczbą danych, jednak istotny jest wyłącznie fakt, że dyrekcja biblioteki zapewnia – zgodnie z normą PN-ISO/IEC 27002:2014-12 – określenie „wytycznych oraz wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz normami prawnymi i regulacjami". Na tym etapie jest to szczególnie cenne, ponieważ pozwala na wykonanie opisu rzeczywistego stanu zasobów. Analizę rozpoczynamy od sprostania wymogom opisanym w normie PN-ISO/IEC 27001:2014-12 w punktach 4.1 „Zrozumienie organizacji i jej kontekstu" oraz 4.2 „Zrozumienie potrzeb i oczekiwań stron zainteresowanych". W tej części analizy bierzemy pod uwagę misję uczelni oraz biblioteki, strukturę organizacyjną uczelni i powiązaną z nią budowę systemu biblioteczno-informacyjnego, stan realizowanych przez książnicę usług informacyjno-bibliotecznych oraz regulamin organizacyjny biblioteki. Ważnym czynnikiem jest także uczelniana polityka bezpieczeństwa informacji oraz powiązany z nią nadrzędny dla nas System Zarządzania Bezpieczeństwem Informacji. Nie wolno również zapomnieć o tym, że mogą istnieć szczególne przypadki, gdy korzysta-

jąc z zapisów normy PN-ISO/IEC 27001:2014-12 w punkcie 4.3 „Określenie zakresu systemu zarządzania bezpieczeństwem informacji", kierujący instytucją podjęli decyzję, że na pewnym etapie działania organizacji, systemem zarządzania bezpieczeństwem informacji należy objąć tylko fragment jej działalności. Stało się tak np. na Uniwersytecie Śląskim w lutym 2014 r. (Zarządzenie, 2014). Oczywiście podjęcie takiej decyzji nie wyklucza objęcia bibliotecznym SZBI innych dodatkowych obszarów informacyjnych, nieobjętych systemową ochroną w ramach całej uczelni. Analogicznie przebiega przygotowanie całościowego SZBI biblioteki publicznej, kiedy jej organ założycielski lub ją nadzorujący będzie miał wdrożone częściowe SZBI. Ważne jest natomiast, by zgodnie z normą PN-ISO/IEC 27001:2014-12 pkt 5.2, na każdym etapie wdrażania systemu PBI była „dostępna jako udokumentowana informacja" oraz „zakomunikowana w organizacji", a także po osiągnięciu odpowiedniego poziomu dojrzałości „dostępna dla stron zainteresowanych, jeśli to jest właściwe". Należy zwrócić uwagę, że normodawca zastrzegł: „jeśli to właściwe", dopuszczając przypadki, gdy polityka bezpieczeństwa zawiera sformułowania, których ujawnienie nie leży w interesie instytucji, ponieważ np. może skutkować zmniejszeniem się poziomu bezpieczeństwa. Kompletna polityka bezpieczeństwa powinna bowiem zawierać opis procedur: organizacji bezpieczeństwa, klasyfikacji i kontroli zasobów, bezpieczeństwa fizycznego i środowiskowego, bezpieczeństwa osobowego, zarządzania systemem komputerowym i siecią oraz kontroli zgodności z prawem.

Po sformułowaniu wstępnej wersji polityki bezpieczeństwa, trzeba przystąpić do inwentaryzacji zasobów, które zostaną objęte SZBI. Zasoby te stanowią zbiory informacji oraz urządzeń technicznych służących do przetwarzania lub dostępu do zbiorów informacji, które należy objąć ochroną w systemie oraz, co bardzo ważne, ludzi, którzy uczestniczą w eksploatacji zasobów informacyjnych.

Ryzyko

Inwentaryzacja wszystkich zasobów jest niezbędna do podjęcia działań opisanych w normie PN-ISO/IEC 27001:2014-12 w punkcie 6.1 „Działania odnoszące się do ryzyk i szans". Opisane w normie PN-ISO/IEC 27005:2010 podejście do szacowania ryzyka pozwala na przygotowanie prostego modelu działań, jakie winno się podejmować, by zapewnić prawidłowe działanie instytucji. „Prawidłowe" dla bibliotek, w tym kontekście oznacza zgodne z obowiązującym prawem zewnętrznym i wewnętrznym (np. zarządzeniami rektora czy dyrektora biblioteki) oraz całkowicie zapewniające realizację usług informacyjno-bibliotecznych ujętych w regulaminach, a także w tradycyjnych i elektronicznych materiałach informacyjnych opisujących instytucję. W ogólności na potrzeby analizy ryzyka cały

model opisu działań, jaki będzie realizowany w przyszłości, można przedstawić w bardzo prosty sposób. Przygotowana wcześniej inwentaryzacja zasobów informacyjnych służy do przyporządkowania im podatności, które powodują, że zgromadzone dane mogą ulec uszkodzeniu lub utracie. Biorąc pod uwagę, że zasoby informacyjne posiadają różną ważność, a podatności takie mogą posiadać bardzo różny poziom, jesteśmy zobowiązani do tego, by przeanalizować, jakie czynności należy podjąć, by działanie biblioteki było nieprzerwane. Oczywiście, jeśli iloczyn wagi i podatności jest znikomy, wtedy najczęściej nie podejmuje się żadnych działań wykraczających poza pewien standard dobrych praktyk. Z reguły istnieje jednak wiele sfer, w których niezbędne jest przygotowanie zabezpieczeń zapewniających bezpieczne działanie systemów informacyjnych. Działanie tych systemów w ogólności ma doprowadzić do tego, by poziom ryzyka wynikający z występujących zagrożeń zewnętrznych i wewnętrznych był akceptowalny, przy równoczesnym spełnieniu wymogów prawa i optymalnych kosztach ich realizacji. Jedną z technik redukcji ryzyka jest jego przenoszenie. Może ono polegać również na wykorzystaniu zasobów innych jednostek organizacyjnych uczelni lub zleceniu zadań związanych z systemami przetwarzającymi informacje instytucjom trzecim. Przy podejmowaniu takich działań należy przeanalizować, czy są one zgodne z obowiązującymi uregulowaniami prawnymi (np. przekazywanie zbiorów danych osobowych do systemów pracujących w chmurach obliczeniowych o nieokreślonej lokalizacji fizycznej). Należy zwrócić uwagę na to, że niejednokrotnie wewnętrzne wymagania instytucji mogą być zdecydowanie mniejsze niż te, które spełniają w całości zapisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji (Rozporządzenie, 2004) czy wydawanych, bądź nowelizowanych na bieżąco ustaw dotyczących działalności gospodarczej, które pośrednio wpływają na bezpieczeństwo systemów informacyjnych.

Zasoby

Tworząc politykę bezpieczeństwa, nie wolno zapomnieć, że właściwe rezultaty przy opracowaniu i wdrażaniu SZBI można osiągnąć tylko wtedy, kiedy w sposób właściwy przygotuje się w bibliotece dane wymagane w normie PN-ISO/IEC 27001:2014-12 w punkcie 6.2 „Cele bezpieczeństwa informacji i planowanie ich osiągnięcia". W praktyce istotne jest, by określić: „co ma być zrobione, jakie zasoby są wymagane, kto będzie odpowiedzialny, kiedy będzie to zakończone oraz jak będą oceniane wyniki". Na tym etapie ważne są kompetencje osób, które angażuje się w przygotowanie SZBI. Dość powszechna opinia, że dla realizacji opracowania i wdrożenia SZBI niezbędne jest zaangażowanie zewnętrznego personelu, nie wydaje się słuszna. Uważamy, że lepiej to zrobią pracownicy znający bibliotekę „od podszewki", którym dostarczono podstawowej wiedzy na temat SZBI.

Można natomiast przyjąć, że osoby z zewnątrz bardziej prawidłowo ocenią kompletność naszej dokumentacji. Powinniśmy również sobie uświadomić, że istnieją także inne metodyki wdrażania SZBI (np. bardzo popularna Information Technology Infrastructure Library – ITIL –Flasiński, 2013), jednak instytucjom publicznym nie pozostawiono innej ścieżki działania niż normy PN-ISO (Rozporządzenie, 2012).

Ważnym aspektem stosowania w praktyce SZBI są działania dotyczące zasobów ludzkich, postrzeganych jako element systemu bezpieczeństwa informacji. W przypadku bibliotek jest to szczególnie ważny czynnik, który wpływa na organizację bezpieczeństwa informacji.Biblioteki naukowe, w szczególności te, które realizują idee biblioteki otwartej – a taka jest CINiBA (Centrum Informacji Naukowej i Biblioteka Akademicka w Katowicach), przyjmują model pracy sprzeczny w praktyce z „podstawowymi kanonami" zapewnienia bezpieczeństwa systemów polegającymi na ograniczaniu dostępu do sprzętu i oprogramowania. Oczywiście sprzeczność ta jest pozorna, a niezwykle ważny staje się odpowiedni poziom wiedzy bibliotekarzy, pracowników informacji naukowej i personelu inżynieryjnego, w tym kadr informatycznych. Kluczowe dla przygotowania i wdrożenia odpowiednich dla bibliotek rozwiązań organizacyjnych i technologicznych, działających w powiązaniu z systemem zarządzania personelem, są zapisy normy PN-ISO/IEC 27001:2014-12 w punktach 7.3 „Uświadamianie", 7.4 „Komunikacja" i 7.5 „Udokumentowane informacje" oraz normy 27002 w punkcie 7.1.2 „Warunki zatrudniania". Tylko odpowiednio dobrany i przeszkolony personel biblioteki zapewni dostarczanie systemów informatycznych, które umożliwiają pełny dostęp do wiedzy gromadzonej w ramach zasobów informacyjnych Internetu. Oczywiście należy pamiętać o tym, że zgodnie z zapisami normy PN-ISO/IEC 27002:2014-12 w punkcie 7.2.2 w ciągu całego okresu zatrudnienia zobowiązani jesteśmy do „uświadamiania, kształcenia i szkolenia z zakresu bezpieczeństwa informacji". W najprostszych formach szkolenia te ograniczają się do wiedzy formalnej, związanej z ochroną danych osobowych, lecz powinny być również uzupełniane o elementy wynikające z wiedzy o zachowaniach społecznych, omawianych np. w książce *Sztuka podstępu. Łamałem ludzi nie hasła* (Mitnick, Simon, 2003). Należy pamiętać, że jednym z elementów zarządzania zasobami ludzkimi jest ściśle zdefiniowany i opisywany w normie ISO/IEC 27002:2014-12 w pkt. 7.2.3 system postępowań dyscyplinarnych. Najważniejsze w tym systemie jest „poprawne i obiektywne traktowanie pracowników" podejrzewanych o naruszenie bezpieczeństwa informacji. Norma zaleca „stosowanie procesu dyscyplinarnego jako środka odstraszającego, aby zapobiec naruszaniu przez pracowników polityki bezpieczeństwa informacji". W związku z tym, podczas przygotowania odpowiednich procedur postępowania należy pamiętać, że pracownicy bibliotek, w strefach przeznaczonych dla czytelników, niejednokrotnie będą musieli działać intuicyjnie, dostosowując zdefi-

niowane schematy do aktualnych zachowań użytkowników sprzętu i systemów teleinformatycznych. Zachowania te, niejednokrotnie nietypowe, mogą zaskakiwać pracowników i nie znajdować odpowiedników we wcześniej zdefiniowanych procedurach.

Podczas przygotowań konkretnych rozwiązań dla instytucji należy korzystać z wcześniej zinwentaryzowanych zasobów, omawianych w normie ISO/IEC 27002:2014-12 pkt. 3 „Aktywa związane z informacjami i środkami przetwarzania informacji". W szczególności „zaleca się, aby inwentaryzacja aktywów była dokładna, aktualna i dostosowana do innych spisów". W bibliotekach, jednym z tych spisów jest raport inwentaryzacji aktywów w powiązaniu ze świadczonymi przez jej agendy usługami informacyjno-bibliotecznymi. Przygotowanie aktywów zgodnie z tą konwencją pozwoli ściśle zlokalizować zarówno systemy do świadczenia usług informacyjno-bibliotecznych, jak również nadmiarowe. W przypadku wykrycia systemów nadmiarowych konieczne jest podjęcie decyzji o ich dalszym utrzymywaniu oraz zbadanie czy koszty zapewnienia bezpieczeństwa nie stanowią zbędnych w skali organizacji wydatków. Podczas inwentaryzacji aktywów informacyjnych należy wskazać ich właścicieli (najczęściej nie będą to działy informatyczne) oraz zdefiniować ich „akceptowalne użycie". Elementy te opisywane są najczęściej proceduralnie i nie zawsze przygotowane systemy zabezpieczeń muszą blokować technicznie dostęp do systemów przetwarzających informacje.

Kontrola dostępu

Instytucje normalizacyjne uznają za jedną z najważniejszych sprawę dostępu – kwestię tę uregulowały w normie ISO/IEC 27002:2014-12 w obszernym rozdziale 9. „Kontrola dostępu". Proces kontroli dostępu jest opisany jako jeden z elementów prowadzenia działalności biznesowej, czyli dla bibliotek – świadczenia usług informacyjno-bibliotecznych. Polityka kontroli dostępu, oprócz spełniania wielu wymienionych w normie elementów formalnych, musi zostać przygotowana tak, by zapewnić bibliotece pełnienie jej podstawowej roli, jaką jest świadczenie usług na rzecz czytelników. Niemożliwa jest realizacja zalecenia normy, że „wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone". Biblioteki najczęściej muszą samodzielnie identyfikować ewentualne zagrożenia i im przeciwdziałać. Zasady organizacji pracy w bibliotekach oraz konieczność odgrywania różnych ról przez jej pracowników powodują, że trudne do spełnienia są również opisane zasady „wiedzy koniecznej" oraz „potrzeby koniecznej"[2]. Najczęściej w zależności od sytuacji i bieżących potrzeb instytucji, bibliotekarze pracują na różnych stanowiskach, korzystając z grafików godzinowych, a pełnione przez nich

[2] „Wiedza konieczna" – oznacza, że pracownik w ramach realizacji zadań służbowych posiada dostęp jedynie do zasobów i informacji, które są mu niezbędne do ich wykonania, a „potrzeba konieczna" to taka, która wynika z konieczności zrealizowania powierzonego zadania.

funkcje zazębiają się. Szczupłość personelu powoduje, że bardzo trudne jest oddzielenie zadań, które powinny być wykonywane na zapleczu w tzw. strefach bezpiecznych od tych, które są wykonywane w strefach otwartych dla czytelników i powinny zostać ograniczone do wąskiego katalogu czynności informacyjnych. Organizacja pracy biblioteki wymaga szczególnej staranności przy tworzeniu systemów zarządzających prawami dostępu do elementów systemów, przeglądania praw dostępu oraz dostosowywania i odbierania praw dostępu. Wszyscy pracownicy biblioteki wykonujący swoje zadania w strefach czytelniczych powinni być pewni, że przydzielone im uprawnienia oraz struktura eksploatowanych systemów wspomagających przetwarzanie informacji zostały dobrane tak, aby praca przebiegała zgodnie z przygotowanymi procedurami i instrukcjami użytkowania, zabezpieczając nie tylko same systemy, lecz także ograniczając (najczęściej nieświadome) zachowania narażające na szwank bezpieczeństwo informacji.

Pisząc o zarządzaniu zasobami ludzkimi, dotknęliśmy już części problemów opisywanych w normie ISO/IEC 27002:2014-12 w rozdziale 11 „Bezpieczeństwo fizyczne i środowiskowe". Część spośród umieszczonych tam zaleceń trudno zrealizować w bibliotece. Problematyczne w wielu lokalizacjach staje się wyznaczenie ścisłej granicy obszaru bezpiecznego, najczęściej nie ma możliwości skutecznego, fizycznego zabezpieczania wejść, a w instytucjach, gdzie udaje się wyznaczyć granice stref czytelniczych i pracowniczych, systemy organizacji pracy i rodzaj kontaktów, jakie muszą utrzymywać bibliotekarze z czytelnikami, tworzą w praktyce strefy półotwarte. Bezużyteczne stają się wówczas zalecenia tworzenia procedur pracy w obszarach bezpiecznych, gdyż takie występują tylko i wyłącznie w wydzielonych pomieszczeniach służb informatycznych lub w samych serwerowniach. W praktyce wszystkie stanowiska, w tym te zlokalizowane w pomieszczeniach służbowych bibliotekarzy, powinny być traktowane równoważnie i przyporządkowywane do stref otwartych.

Zarządzanie sprzętem

Osobnego omówienia wymaga postępowanie ze sprzętem służącym do przetwarzania informacji. Sprzęt ten dzielimy na dwie grupy: ten zgromadzony w serwerowni i ten używany bezpośrednio przez pracowników biblioteki. Sprzęt pracujący w serwerowni przygotowany jest do pracy ciągłej. Zapewniając mu właściwe, stabilne warunki temperaturowe i wilgotnościowe oraz specjalne plany serwisowe, spełniamy większość wymagań przewidzianych w normach. Sprzęt użytkowany bezpośrednio przez pracowników biblioteki to prawie zawsze komputery osobiste, do których dostęp mają nie tylko ich użytkownicy. Zlokalizowane na terenie całej biblioteki, również w strefach otwartych dla czytelników, są narażone nie tylko na zmienne warunki atmosferyczne, lecz także na bezpośrednią ingerencję osób nie-

uprawnionych (firmy lub personel sprzątający, ochrona czy konserwatorzy niezwiązani z biblioteką). Działając zgodnie z wymogami normy, winniśmy tak organizować systemy przetwarzające informacje, by były one w nich bezpieczne, m.in. poprzez lokowanie systemów na sprzęcie, do którego dostęp mają wyłącznie osoby upoważnione do przetwarzania informacji. Należy tak przygotować rozwiązania organizacyjne i systemy komputerowe, by na stacjach ogólnodostępnych nie były fizycznie lokowane dane pochodzące z systemów informacyjnych podlegających szczególnej ochronie. W bibliotekach należy przyjąć, że sprzęt zlokalizowany w strefach przeznaczonych dla czytelników (nawet ten, który użytkują pracownicy biblioteki) oraz ten w strefie pracowniczej, gdzie pojawiają się obsługiwani przez bibliotekarzy czytelnicy, powinien być traktowany zgodnie z zapisami normy ISO/IEC 27002:2014-12 punkt 11.2.6 „Bezpieczeństwo sprzętu i aktywów poza firmą". Sprzęt tak traktowany pozostaje również bezpieczny, kiedy powstaje konieczność przesunięcia go w inne miejsce, innego wykorzystania lub konieczność jego zbycia (27002:2014-12 pkt 11.2.7).

W bibliotekach, w których wyznaczono strefy wolnego dostępu dla czytelników (choćby to była nawet mała czytelnia), istotne jest właściwe gospodarowanie systemami okablowania opisanymi w normie ISO/IEC 27002:2014-12 pkt 11.2.3 „Bezpieczeństwo okablowania". Ważne jest stosowanie technik zapobiegających przechwyceniu transmisji danych. Ponieważ niemożliwe jest spełnienie warunku kontrolowanego dostępu do paneli połączeniowych (w szczególności tych rozproszonych w otwartych strefach czytelniczych), należy stosować takie rozwiązania technologiczne, które będą skutecznie zapobiegały możliwości podłączania obcego sprzętu w celu prowadzenia nasłuchu transmisji danych.

Zasady organizacyjne

Zapewnienie bezpiecznej eksploatacji systemów przetwarzających informacje w chronionym przez nie zakresie to zagadnienie bardzo obszerne. Działania prowadzi się w zakresie organizacji pracy całej instytucji, a także poszczególnych systemów informacyjnych wspomagających jej pracę. Z jednej strony zgodnie z normą ISO/IEC 27002:2014-12 punkt 12.1.1 zaleca się, by opracować dokumentację wszystkich procesów eksploatacyjnych systemów przetwarzających informacje, z drugiej, w punkcie 12.1.2 przypomina o zarządzaniu zmianami w eksploatowanych systemach. W szczególności należy opracować dokumentację instalacji i konfiguracji systemów, przetwarzania i postępowania z informacją (automatycznego jak i ręcznego), kopii zapasowych wraz z procedurami ponownego uruchamiania i odtwarzania systemów z kopii zapasowych, a także procedur monitorowania. Równocześnie, w zakresie zarządzania zmianami, szczególnie ważne w bibliotekach jest planowanie i testowanie wszystkich wprowadza-

nych zmian wraz z procesami ich zatwierdzania. Dotyczy to w szczególności systemu zintegrowanego, który jest podstawowym systemem automatyzującym pracę instytucji. W przypadku CINiBA, tylko sprawne jego działanie pozwala m.in. na bezbłędne lokalizowanie dokumentów w strefach wolnego dostępu i magazynach zamkniętych oraz stałe monitorowanie drogi książki między agendami biblioteki. W związku z tym niebagatelne jest przygotowanie „procedur przywracania, w tym procedur i odpowiedzialności za przerwanie i odtworzenie na wypadek niepomyślnych zmian lub nieprzewidzianych zdarzeń". Działania te są domeną służb informatycznych (w szczególności Administratorów Bezpieczeństwa Informacji) oraz osób odpowiedzialnych za jakość usług świadczonych przez biblioteki.

Dla zapewnienia pełnego bezpieczeństwa danych gromadzonych w systemach informacyjnych norma ISO/IEC 27002:2014-12 w punkcie 12.1.4 zaleca „Oddzielenie środowisk rozwojowych, testowych i produkcyjnych". Małe biblioteki eksploatujące takie systemy – ze względów oszczędnościowych – rzadko podejmują decyzje o eksploatacji systemów rozwojowych i testowych. Zjawisko to dotyczy również systemów informatycznych obsługujących biblioteki w uczelnianych i regionalnych centrach obliczeniowych. Brak instalacji rozwojowych można uzasadniać tym, że oprogramowanie jest testowane przez producentów w procesie produkcji i to właśnie te firmy odpowiadają za jego jakość, należy jednak podkreślić, że nieobecność systemów testowych oraz procedur testowania nowych wersji oprogramowania w swoich ryzykach obciąża bezpośrednio zarządzających bibliotekami. Najczęściej sytuacja ta odnosi się do bibliotek pozbawionych wysoko wykwalifikowanej kadry informatycznej lub systemu zarządzania jakością świadczonych usług. W celu zachowania pełnego bezpieczeństwa, systemy te powinny być rozdzielane poprzez sadowienie ich na różnych serwerach, a także stosowanie oddzielnych profili pracy bibliotekarzy dla środowisk testowych i produkcyjnych. Testy w systemach produkcyjnych można uruchamiać tylko w sytuacjach wyjątkowych. Ważne jest sprawne i bezawaryjne odtworzenie zasobów informacyjnych z wcześniej przygotowanych kopii zapasowych; służą temu celowi przygotowane wcześniej procedury tworzenia i testowania procesu zabezpieczania danych. Szczególnej ochronie (również w zakresie tworzenia kopii zapasowych) podlegają systemowe rejestry zdarzeń zawierające również rejestry działań administratorów i operatorów. Z kopiami zapasowymi powiązane są także strategie instalacji nowych wersji oprogramowania w systemach produkcyjnych, które powinny obejmować zarówno aktualizacje zakończone powodzeniem, jak i sytuacje awaryjne, kiedy niezbędne jest przywrócenie poprzednich ich wersji. Istotne w tych działaniach jest wcześniejsze przeprowadzenie próby migracji z wykorzystaniem systemu testowego. Biblioteki, mimo zaleceń normatywnych o konieczności użytkowania oprogramowania wspieranego przez jego producentów często używają starych systemów, pozbawionych takiego

wsparcia, tłumacząc się brakiem funduszy na nowe ich wersje. Argumenty te rzadko są weryfikowane w powiązaniu z zakresem i poziomem świadczonych usług oraz metodologią TCO w analizie rynkowej kosztów instytucji. Warto podkreślić, iż zagadnienia związane z kolejnymi wersjami oprogramowania użytkowego ujmuje norma ISO/IEC 27002:2014-12 w rozdziale 14 „Pozyskiwanie, rozwój i utrzymanie systemów", która „zaleca […] włączyć wymagania dotyczące bezpieczeństwa informacji do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących". Należy pamiętać również o aktualizowaniu systemów operacyjnych serwerów i stacji roboczych. Oprogramowanie aktualizacyjne powinno być pobierane z pewnych źródeł, a sam proces aktualizacji przeprowadzany bez zbędnej zwłoki. Służbom informatycznym bibliotek zaleca się przeprowadzanie procedur aktualizacyjnych bez zaburzania pracy samej instytucji. Obowiązkiem normatywnym wynikającym z ISO/IEC 27002:2014-12 pkt. 12.2 jest również zapewnienie ochrony przed szkodliwym oprogramowaniem. Dotyczy to wirusów, instalowania oprogramowania antywirusowego oraz innych możliwych zależnych od rodzaju instytucji działań technicznych, na które powinny zostać przygotowane odpowiednie do potrzeb procedury postępowania.

Podatności i audyt

Kolejnym bardzo ważnym zagadnieniem jest zarządzanie podatnościami technicznymi omawiane w normie ISO/IEC 27002:2014-12 pkt 12.6. Działania w tym zakresie muszą być realizowane względem urządzeń technicznych, głównie elektronicznych oraz oprogramowania nimi sterującego. Dotyczą w różnym zakresie uszkodzeń technicznych nośników, na których przechowywane są chronione informacje, jak również wszystkich elementów do przetwarzania i przesyłania tych danych. Zarządzający bibliotekami zobowiązani są do przygotowania konfiguracji i procedur eksploatacyjnych zapewniających dostęp do świadczonych usług informacyjno-bibliotecznych na założonym, akceptowalnym przez władze uczelni poziomie. W celu zagwarantowania niezawodnej pracy systemów biblioteki są zobowiązane do wprowadzenia (nie tylko ze względów licencyjnych) ograniczeń w zakresie instalowania i uruchamiania oprogramowania, głównie na stacjach roboczych oraz tych serwerach, na których w ramach sesji aplikacyjnych pracuje oprogramowanie przetwarzające dane do systemów informacyjnych. Zapisy normy ISO/IEC 27002:2014-12 w rozdziale 13 „Bezpieczeństwo komunikacji" zalecają stosowanie w miarę potrzeb szyfrowanego przesyłania danych, a także rozdzielenie sieci służących dla różnych celów lub wykorzystywanych przez różnych użytkowników. Ponadto definiują zasady tworzenia procedur przesyłania informacji, łącznie z warunkami zawierania porozumień w tym zakresie. W przypadku CINiBA są to np. porozumienia o wzajemnym powierzeniu danych osobowych zawarte pomiędzy Uni-

wersytetem Śląskim i Uniwersytetem Ekonomicznym w Katowicach, które również podlega innym uregulowaniom ustawowym (Ustawa, 1997).

Ważną rolę odgrywa również zabezpieczenie audytu systemów informacyjnych opisane w normie ISO/IEC 27002:2014-12 pkt 12.7, realizowane na podstawie normy PN-ISO/IEC 27005:2014-01 (Technika informatyczna, 2014b) i Rozporządzenia RM (Rozporządzenie, 2012). Działania audytorów wewnętrznych powinny być prowadzone dwojako: jako zadania zlecone przez instytucje nadzorujące uczelnie wyższe oraz prace samodzielnie planowane i kwalifikowane jako doradcze. Audyt powinien obejmować w coraz szerszym zakresie systemy teleinformatyczne, które mogą być angażowane w przyszłości do przetwarzania informacji podlegających szczególnej ochronie.

Za najważniejsze wdrożone i możliwe do upublicznienia rozwiązania związane z bezpieczeństwem CINiBA należą: „opieka" nad systemami operacyjnymi i aplikacjami użytkowymi stacji roboczych i serwerów aplikacyjnych, stworzenie systemu uprawnień dostępowych (stacje robocze i aplikacje), publikowanie aplikacji, „mrożenie" systemów operacyjnych stacji roboczych czytelników, stosowanie systemu dostępu do sieci fizycznej i bezprzewodowej (dedykowane podsieci), ochrona antywirusowa, posiadanie odpowiedniego systemu archiwowania zasobów z polityką przechowywania archiwów.

Podsumowanie

Współczesna technologia i wdrażane zasady organizacji pracy przesuwają na systemy informacyjne, oparte najczęściej na systemach informatycznych, znaczną odpowiedzialność za jakość działania instytucji. Sytuacja ta nakłada na zarządzających istotną odpowiedzialność za właściwą organizację bezpieczeństwa. Działania, które podejmować muszą w ramach codziennych czynności zarządczych, wymagają ciągłego kształcenia, niezbędnego do zapewnienia prawidłowego funkcjonowania organizacji. Należy pamiętać, że wszystkie omówione działania powinny być podejmowane w każdej z omówionych sfer organizacji pracy[3].

Bibliografia

Koziara A., Jezierska, A. (2015). Bezpieczeństwo danych i systemów informacyjnych w bibliotekach. Przegląd stanu prawnego. *Bibliotheca Nostra. Śląski Kwartalnik Naukowy*, 4, 41-53.

Krawiec J., Ożarek G. (2014). *System Zarządzania Bezpieczeństwem Informacji w praktyce.* Wyd. 2 zaktual. i uzup. Warszawa: PKN.

[3] Opracowano m.in. na podstawie: Flasiński M., (2013). *Zarządzanie projektami informatycznymi.* Warszawa: Wydawnictwo Naukowe PWN.

Mitnick, K., Simon, W. (2003). *Sztuka podstępu*. Gliwice: Wydawnictwo Helion.

(Rozporządzenie, 2004). Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004, nr 100, poz. 1024).

(Rozporządzenie, 2012). Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526 z późn. zm.).

(Technika informatyczna, 2007a) Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania PN-ISO/IEC 27001:2007 - wersja polska. (2007) zastąpiona przez PN-ISO/IEC 27001:2014-12 Warszawa: PKN.

(Technika informatyczna, 2007b). Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji PN-ISO/IEC 17799:2007 – wersja polska. (2007). Warszawa: PKN.

(Technika informatyczna, 2014a). Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania PN-ISO/IEC 27001:2014-12 – wersja polska. (2014). Warszawa: PKN.

(Technika informatyczna, 2014a). Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji PN-ISO/IEC 27002:2014-12 – wersja polska. (2014). Warszawa: PKN.

(Technika informatyczna, 2014b) Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji PN-ISO/IEC 27005:2014-01 – wersja polska. (2014). Warszawa: PKN.

(Systemy zarządzania jakością, 2009). Systemy zarządzania jakością – Wymagania PN-EN ISO 9001:2009 – wersja polska. (2009). Warszawa: PKN.

(Systemy zarządzania jakością, 2015). Systemy zarządzania jakością – Wymagania PN-EN ISO 9001:2015-10 – wersja angielska. (2015). Warszawa: PKN.

(Ustawa, 1997). Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. 2014, poz. 1182 z późn. zm.).

(Zarządzenie, 2014) Zarządzenie Rektora Uniwersytetu Śląskiego nr 16/2014 w sprawie wprowadzenia do użytku służbowego Polityki Bezpieczeństwa w Zakresie Ochrony Danych Osobowych w Uniwersytecie Śląskim w Katowicach oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Uniwersytecie Śląskim w Katowicach.

Andrzej Koziara, Agnieszka Jezierska

Selected practical aspects of providing security of IT systems in the light of the applicable standards

Summary

Providing practical security to the IT systems is a complicated process resulting from legal and standard regulations. The study describes elements connected with establishment and implementation of the security policy and practical activities performed on its basis. It takes into account all aspects related with organizational changes each institution undergoes, when working with security rules procedures.

Special attention is paid to practical aspects of risk analysis and activities resulting from conducted studies, including crisis support schemes. The paper describes the most important measures undertaken by the University of Silesia in order to provide activities which are compliant with the current legal bills and international standard acts. It also discusses some elements associated with the work organization, including investment activities performed according to the principles resulting from the analysis of total costs calculated according to the Total Cost of Ownership (TCO) model.

Keywords: ICT security, risk analysis, security policy, modern scientific libraries